



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/692,884	10/20/2000	Kenneth R. Owens	069116.0172	6113
5073	7590	11/14/2007		
BAKER BOTTS L.L.P. 2001 ROSS AVENUE SUITE 600 DALLAS, TX 75201-2980			EXAMINER MATTIS, JASON E	
			ART UNIT 2616	PAPER NUMBER
			NOTIFICATION DATE 11/14/2007	DELIVERY MODE ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ptomail1@bakerbotts.com
glenda.orrantia@bakerbotts.com



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

MAILED
DEC 09 2007
GROUP 2600

**BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES**

Application Number: 09/692,884
Filing Date: October 20, 2000
Appellant(s): OWENS ET AL.

Charles S. Fish
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 8/20/07 appealing from the Office action mailed 8/22/06.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

US 2002/0181485 A1	Cao et al.	12-2002
US 6,697,329 B1	McAllister et al.	2-2004
US 6,590,893 B1	Hwang et al.	7-2003

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 10-11 and 13-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cao et al. (U.S. Publication US 2002/0181485 A1) in view of McAllister et al. (U.S. Pat. 6697329).

With respect to claim 10, Cao et al. discloses a multi-protocol label switching system comprised of a plurality of data switches, label switching routers, that are

interconnected by a plurality of data paths from a source node, LSR S, to a destination node, LSR E, through the data switches, LSR A and LSR B (**See paragraph 22 and Figure 1 of Cao et al. for reference to an MPLS data network comprised of label switching routers interconnected by paths**). Cao et al. also discloses a method within the MPLS data network of routing a traffic flow from a working path through the network to a protection path through the network (**See paragraph 24 and Figure 1 of Cao et al. for reference to switching to a secondary path when a primary path fails**). Cao et al. further discloses sending a first control message to establish a working data path and a separate protection path for the traffic flow from a first switch, LSR S, to a second switch, LSR E (**See paragraph 23-24 and Figure 1 of Cao et al. for reference to sending a router request downstream to request an explicitly routed path between source LSR S and destination LSR E and for reference to establishing a secondary route between source LSR S and destination LSR E**). Cao et al. does not disclose sending a second message from the second switch to the first switch establishing a reverse notification path through the network between the second and first switches. Cao et al. also does not disclose sending a third message over the reverse notification path from the second switch to the first switch in response to the second switch receiving the traffic from the first switch over the working path, the interruption of which controls protection switching by the first switch.

With respect to claim 10, McAllister et al., in the field of communications, discloses sending a message establishing a reverse notification path through the network between the first and second switches (**See column 9 line 47 to column 10**

line 8 of McAllister et al. for reference to using a path from a second node to a first node to sending messages and acknowledgements to the message from the second node to the first node in response to protocol messages, the second message, sent from the first node). McAllister et al. also discloses sending a third message over the reverse notification path from the second switch to the first switch in response to the second switch receiving the traffic from the first switch over the working path, the interruption of which controls protection switching by the first switch **(See column 9 line 47 to column 10 line 8 of McAllister et al. for reference to the messaging being in an acknowledgement format, meaning that a third acknowledgement message is sent from the second node in response to receiving a message, which is in a traffic flow from the first node over a working virtual connection).** Setting up a reverse notification path and sending signals over the path to a first, source, node has the advantage of allowing a first, source, node to learn about a failure in a data path and immediately stop sending packets that will be “lost” on the failed path before the source node switches to the secondary path and also allowing the source node to resend packets on the secondary path that may have been “lost” while the destination node was receiving packets through the failed path.

It would have been obvious to one of ordinary skill in the art at the time of the invention, when presented with the work of McAllister et al., to combine setting up a reverse notification path and sending signals over the path to a first node to allow the first node to control protection switching, as suggested by McAllister et al., with the MPLS protection path system of Cao et al. with the motivation being to allow a first,

Art Unit: 2616

source, node to learn about a failure in a data path and immediately stop sending packets that will be "lost" on the failed path before the source node switches to the secondary path and also allow the source node to resend packets on the secondary path that may have been "lost" while the destination node was receiving packets through the failed path.

With respect to claim 11, Cao et al. discloses that sending a first message is comprises adding a protection messaging field, which carries protection pathway information between switching elements, to a label distribution protocol message (**See column 24 and Figure 1 of Cao et al. for reference to using label distribution protocol to establish label switching paths to set up primary and protection data paths**).

With respect to claim 13, Cao et al. discloses that sending a first predetermined control message from a first switch to a second switch comprises includes identifying at least one switch as a protection switch element, LSR C and LSR D, by the contents of at least one control field sent to at least one switch, LSR E (**See paragraphs 23-24 and Figure 1 of Cao et al. for reference to LSR S using control fields to identify LSR C and LSR D as protection switch elements and sending this control information through the network to LSR E**).

With respect to claim 14, Cao et al. discloses the working path being set up loosely (**See paragraph 2 of Cao et al. for reference to prior art using loosely connected working and protection paths set up hop-by-hop**).

With respect to claim 15, Cao et al. discloses the working path being set up explicitly (See paragraph 21 of Cao et al. for reference to explicitly setting up working and protection routing paths).

With respect to claim 16, Cao et al. discloses mapping labels to the traffic flow routed along the working path according to predetermined criteria that includes the quality of service granted to the traffic flow (See paragraph 53 and Figure 2 of Cao et al. for reference to mapping labels routed along the first path according to predetermined criteria including a type of service field, which includes quality of service information).

With respect to claim 17, Cao et al. discloses a system for establishing a traffic flow over a protection path in a data network (See paragraph 24 and Figure 1 of Cao et al. for reference to switching to a secondary path when a primary path fails). Cao et al. also discloses a plurality of switches, label switching routers, operable to route the traffic flow in the data network **(See paragraph 22 and Figure 1 of Cao et al. for reference to the communications system including label switching routers that use paths to route a traffic flow).** Cao et al. further discloses a first one of switches, LSR S, operable to establish a working path and a protection and a second one of the plurality of switches, LSRs A, B, and E, that is downstream from the first switch being on the working path **(See paragraph 23-24 and Figure 1 of Cao et al. for reference to sending a router request downstream to request an explicitly routed path between source LSR S and destination LSR E that sets up a working path through LSRs S, A, B, and E, with LSRs A, B, and E downstream from LSR S).**

Cao et al. does not disclose that the second switch is operable to establish a reverse notification path and send a reverse notification message upstream to the first switch in response to receiving the traffic flow from the first switch. Cao et al. also does not disclose a reverse notification message operable to provide information related to the working path in order to determine whether the traffic flow is to be re-routed from the working path to the protection path, the interruption of which controls protection switching.

With respect to claim 17, McAllister et al., in the field of communications, discloses sending a message establishing a reverse notification path through the network between the first and second switches in response to data received from the first switch (See column 9 line 47 to column 10 line 8 of McAllister et al. for reference to using a path from a second node to a first node to sending messages and acknowledgements to the message from the second node to the first node in response to protocol messages, the second message, sent from the first node). McAllister et al. also discloses sending a third message over the reverse notification path the interruption of which is used to determine whether the traffic flow is to be re-routed from the working path to the protection path (See column 9 line 47 to column 10 line 8 of McAllister et al. for reference to the messaging being in an acknowledgement format, meaning that a third acknowledgement message is sent from the second node in response to receiving a message, which is in a traffic flow from the first node over a working virtual connection). Setting up a reverse notification path and sending signals over the path to a first, source, node has

the advantage of allowing a first, source, node to learn about a failure in a data path and immediately stop sending packets that will be “lost” on the failed path before the source node switches to the secondary path and also allowing the source node to resend packets on the secondary path that may have been “lost” while the destination node was receiving packets through the failed path.

It would have been obvious to one of ordinary skill in the art at the time of the invention, when presented with the work of McAllister et al., to combine setting up a reverse notification path and sending signals over the path to a first node to allow the first node to control protection switching, as suggested by McAllister et al., with the MPLS protection path system of Cao et al. with the motivation being to allow a first, source, node to learn about a failure in a data path and immediately stop sending packets that will be “lost” on the failed path before the source node switches to the secondary path and also allow the source node to resend packets on the secondary path that may have been “lost” while the destination node was receiving packets through the failed path.

With respect to claims 18 and 20, Cao et al. does not disclose the first switch being a protection switch element operable to re-route data onto the protection path in accordance with the reverse notification message in response to not receiving the reverse notification message from the second switch within a predetermined time interval.

With respect to claims 18 and 20, McAllister et al. discloses that the first switch is a protection switch element operable to re-route the traffic flow onto the protection

path in accordance with the reverse notification message (**See column 9 line 47 to column 10 line 8 of McAllister et al. for reference to the source or ingress node, which is the first switch, re-routing the connection to a different path and for reference to sending an acknowledgement message, or a third message, which the first node uses, by determining when the acknowledgement message was not received, or interrupted, to control protection switching from the second node to the first node**). Setting up a reverse notification path and sending signals over the path to a first, source, node has the advantage of allowing a first, source, node to learn about a failure in a data path and immediately stop sending packets that will be "lost" on the failed path before the source node switches to the secondary path and also allowing the source node to resend packets on the secondary path that may have been "lost" while the destination node was receiving packets through the failed path.

It would have been obvious to one of ordinary skill in the art at the time of the invention, when presented with the work of McAllister et al., to combine setting up a reverse notification path and sending signals over the path to a first node to allow the first node to control protection switching, as suggested by McAllister et al., with the MPLS protection path system of Cao et al. with the motivation being to allow a first, source, node to learn about a failure in a data path and immediately stop sending packets that will be "lost" on the failed path before the source node switches to the secondary path and also allow the source node to resend packets on the secondary path that may have been "lost" while the destination node was receiving packets through the failed path.

With respect to claims 19 and 21, Cao et al. does not disclose the first switch sending its own reverse notification message including information from the reverse notification message received from the second switch, with the reverse notification message informing the first switch of the status of the second switch and all other switches downstream from the first switch on the working path.

With respect to claims 19 and 21, McAllister et al. discloses a first switch sending and receiving reverse notification messages including the information from the reverse notification messages received from all switches downstream from the first switch on the working path **(See column 9 line 47 to column 10 line 8 of McAllister et al. for reference to the acknowledgement messages sent by the nodes containing signaling messages for all virtual connections associate with a data link, meaning the content of each message is a compilation of the contents of acknowledgement messages from previous nodes, such that the acknowledgement message from the first node contains the information of the acknowledgement message from the second node)**. Sending a reversion notification message including the information from the reverse notification messages received from another switch has the advantage of allowing link status information to be propagated throughout the network so that all switches know the status of all system links.

It would have been obvious to one of ordinary skill in the art at the time of the invention, when presented with the work of McAllister et al., to combine sending a reversion notification message including the information from the reverse notification

messages received from another switch, as suggested by McAllister et al., with the MPLS protection path system of Cao et al. with the motivation being to allow link status information to be propagated throughout the network so that all switches know the status of all system links.

With respect to claims 22-24, Cao et al. does not disclose the second switch sending its reverse notification message directly to each of the switches including the particular switch that performs protection switching from the working path to the protection path with the reverse notification message including information pertaining to a failure in the working path.

With respect to claims 22-24, McAllister et al. discloses switches sending reverse notification messages directly to other switches including the switch that performs protection switching with the reverse notification message including information pertaining to a failure on the working path (**See column 9 line 47 to column 10 line 8 of McAllister et al. for reference to the acknowledgement messages being sent in a “poll” and “stat” format, meaning that a first source node will “poll” the status of a second node and the second node will respond with a “stat” message sent directly to the node that initiated the “poll” message and for reference to the “poll” and “stat” messages containing information pertaining to failures on the working path that is used by the first source node to perform protection switching**). Sending reverse notification messages directly to other switches including the switch that performs protection switching with the reverse notification message including information pertaining to a failure on the working path

has the advantage of allowing the protection switching to be processed and performed by a single specific protection switch without using the resources of the other switches to process each individual reverse notification message.

It would have been obvious to one of ordinary skill in the art at the time of the invention, when presented with the work of McAllister et al., to combine reverse notification messages directly to other switches including the switch that performs protection switching with the reverse notification message including information pertaining to a failure on the working path, as suggested by McAllister et al., with the MPLS protection path system of Cao et al. with the motivation being to allow the protection switching to be processed and performed by a single specific protection switch without using the resources of the other switches to process each individual reverse notification message.

Claims 1-2, 4-5, and 7-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cao et al. (U.S. Publication US 2002/0181485 A1) in view of McAllister et al. (U.S. Pat. 6697329) and in further view of Hwang et al. (U.S. Pat. 6590893).

With respect to claim 1, Cao et al. discloses a multi-protocol label switching system comprised of a plurality of data switches, label switching routers, that are interconnected by a plurality of data paths from a source node, LSR S, to a destination node, LSR E, through a first set of data switches, LSR A and LSR B **(See paragraph 22 and Figure 1 of Cao et al. for reference to an MPLS data network comprised of**

label switching routers interconnected by paths). Cao et al. also discloses a method within the MPLS data network of establishing a data flow over a protection path from a source switch, LSR S, to a destination switch, LSR E, through a second set of switches, LSR C and LSR D **(See paragraph 24 and Figure 1 of Cao et al. for reference to switching to a secondary path when a primary path fails).** Cao et al. further discloses sending a first message to establish a working data path and a protection path for a traffic flow from a first switch, LSR S, to a second switch, LSR E **(See paragraph 23-24 and Figure 1 of Cao et al. for reference to sending a router request downstream to request an explicitly routed path between source LSR S and destination LSR E and for reference to establishing a secondary route between source LSR S and destination LSR E).** Cao et al. does not disclose sending a second message from the second switch to the first switch establishing a reverse notification path through the network between the second and first switches. Cao et al. also does not disclose sending a third message over the reverse notification path in response to the second switch receiving the traffic flow over the working path from the first switch in order to control protection switching by the first switch, with the third message indicating whether the traffic flow sent on the working path was received intact and on time by the second switch.

With respect to claim 1, McAllister et al., in the field of communications, discloses sending a message establishing a reverse notification path through the network between the first and second switches **(See column 9 line 47 to column 10 line 8 of McAllister et al. for reference to using a path from a second node to a**

Art Unit: 2616

first node to sending messages and acknowledgements to the message from the second node to the first node in response to protocol messages, the second message, sent from the first node). McAllister et al. also discloses sending a third message over the reverse notification path in response to the second switch receiving the traffic flow over the working path from the first switch in order to control protection switching by the first switch, with the third message indicating whether the traffic flow sent on the working path was received on time by the second switch **(See column 9 line 47 to column 10 line 8 of McAllister et al. for reference to the messaging being in an acknowledgement format, meaning that a third acknowledgement, message is sent from the second node in response to receiving a message, which is in a traffic flow from the first node over a working virtual connection, and for reference to the acknowledgement messages implementing a keep-alive or heartbeat polling process, meaning that the acknowledgement messages are an indication of whether the traffic is received on time since these messages are sent “constantly” and are therefore expected to be acknowledged “constantly”).**

Setting up a reverse notification path and sending signals over the path to a first, source, node has the advantage of allowing a first, source, node to learn about a failure in a data path and immediately stop sending packets that will be “lost” on the failed path before the source node switches to the secondary path and also allowing the source node to resend packets on the secondary path that may have been “lost” while the destination node was receiving packets through the failed path.

It would have been obvious to one of ordinary skill in the art at the time of the invention, when presented with the work of McAllister et al., to combine setting up a reverse notification path and sending signals over the path to a first node to allow the first node to control protection switching, as suggested by McAllister et al., with the MPLS protection path system of Cao et al. with the motivation being to allow a first, source, node to learn about a failure in a data path and immediately stop sending packets that will be "lost" on the failed path before the source node switches to the secondary path and also allow the source node to resend packets on the secondary path that may have been "lost" while the destination node was receiving packets through the failed path.

With respect to claim 1, although McAllister et al. discloses the use of acknowledgement messages, the combination of McAllister et al. and Cao et al. does not disclose that acknowledgement messages are used as an indication whether the traffic flow sent on the working path was received intact.

With respect to claim 1, Hwang et al., in the field of communications discloses acknowledgement messages that are used as an indication whether a traffic flow was received intact (**See column 7 lines 40-50 of Hwang et al. for reference to an acknowledgement messages that is only sent if data was received without errors, meaning the reception or lack of reception of an acknowledgement message is used as an indication of whether a traffic flow was received without errors, or intact**). Using acknowledgement messages that are used as an indication whether a traffic flow was received intact has the advantage of allowing the quality of a data link to

be signaled from a destination node to a source node such that the source node can determine if data being sent of a path between the source and destination is being received without error.

It would have been obvious for one of ordinary skill in the art at the time of the invention, when presented with the work of Hwang et al., to combine using acknowledgement messages that are used as an indication whether a traffic flow was received intact, as suggested by Hwang et al., with the system and method of Cao et al. and McAllister et al., with the motivation being to allow the quality of a data link to be signaled from a destination node to a source node such that the source node can determine if data being sent of a path between the source and destination is being received without error.

With respect to claim 2, Cao et al. discloses that the step of sending a first message is comprised of the step of adding a protection messaging field, which carries protection pathway information between switching elements, to a label distribution protocol message **(See column 24 and Figure 1 of Cao et al. for reference to using label distribution protocol to establish label switching paths to set up primary and protection data paths)**.

With respect to claim 4, Cao et al. discloses that the step of sending a message to establish a working path and a protection path between the first and second switches, LSR S and LSR E, includes the step of identifying at least one data switch, LSR S, as a switch element by the contents of at least one control field sent to at least one data switch, LSR E, of the MPLS network **(See paragraph 23-24 and Figure 1 of Cao et al.**

for reference to LSR S using control fields sent through the network to LSR E to request an explicitly routed path identifying itself as the source LSR).

With respect to claim 5, Cao et al. discloses that the step of sending a first predetermined message to establish a working path and a protection path between the first and second switches, LSR S and LSR E, includes the step of identifying at least one data switch as a protection switch element, LSR C and LSR D, by the contents of at least one control field sent to at least one data, switch LSR E, of the MPLS network (See paragraphs 23-24 and Figure 1 of Cao et al. for reference to LSR S using control fields to identify LSR C and LSR D as protection switch elements and sending this control information through the network to LSR E).

With respect to claim 7, Cao et al. discloses the working path being set up loosely (See paragraph 2 of Cao et al. for reference to prior art using loosely connected working and protection paths set up hop-by-hop).

With respect to claim 8, Cao et al. discloses the working path being set up explicitly (See paragraph 21 of Cao et al. for reference to explicitly setting up working and protection routing paths).

With respect to claim 9, Cao et al. discloses a step for mapping labels to the traffic flow routed along the working path according to predetermined criteria that includes the quality of service granted to the traffic flow (See paragraph 53 and Figure 2 of Cao et al. for reference to mapping labels routed along the first path according to predetermined criteria including a type of service field, which includes quality of service information).

Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Coe et al. in view of McAllister et al. and Hwang et al. as applied to claims 1-2, 4-5, and 7-9 above, and further in view of Aukia et al. (U.S. Pat. 6594268).

With respect to claim 3, the combination of Cao et al., McAllister et al., and Hwang et al. does not disclose that sending a first message is comprised of the step of adding a protection messaging field, which carries protection pathway information between switching elements, to an MPLS reservation protocol message.

Aukia et al., in the field of communications, discloses that sending a message is comprised of the step of adding a protection messaging field, which carries protection pathway information between switching elements, to an MPLS reservation protocol message (**See column 9 line 60 to column 10 line 47 and Figure 2 of Aukia et al. for reference to control messages using RSVP protocol, which are used to carry protection pathway information between network nodes**). Using an MPLS reservation protocol message to carry protection pathway information between switching elements has the advantage of being able to share protection pathway information between network elements using the current MPLS protocol, meaning that the current MPLS protocol would not have to be changed in order to implement the invention.

It would have been obvious for one of ordinary skill in the art at the time of the invention, when presented with the work of Aukia et al. to combine the use of an MPLS reservation protocol message of Aukia et al. with the MPLS protection path method of

Cao et al., McAllister et al., and Hwang et al., with the motivation being to be able to share protection pathway information between network elements using the current MPLS protocol, meaning that the current MPLS protocol would not have to be changed in order to implement the invention.

Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Coe et al. in view of McAllister et al. as applied to claims 10-11 and 13-24 above, and further in view of Aukia et al. (U.S. Pat. 6594268).

With respect to claim 12, the combination of Cao et al. and McAllister et al. does not disclose that sending a first message is comprised of the step of adding a protection messaging field, which carries protection pathway information between switching elements, to an MPLS reservation protocol message.

Aukia et al., in the field of communications, discloses that sending a message is comprised of the step of adding a protection messaging field, which carries protection pathway information between switching elements, to an MPLS reservation protocol message (**See column 9 line 60 to column 10 line 47 and Figure 2 of Aukia et al. for reference to control messages using RSVP protocol, which are used to carry protection pathway information between network nodes**). Using an MPLS reservation protocol message to carry protection pathway information between switching elements has the advantage of being able to share protection pathway information between network elements using the current MPLS protocol, meaning that

Art Unit: 2616

the current MPLS protocol would not have to be changed in order to implement the invention.

It would have been obvious for one of ordinary skill in the art at the time of the invention, when presented with the work of Aukia et al. to combine the use of an MPLS reservation protocol message of Aukia et al. with the MPLS protection path method of Cao et al. and McAllister et al., with the motivation being to be able to share protection pathway information between network elements using the current MPLS protocol, meaning that the current MPLS protocol would not have to be changed in order to implement the invention.

Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Cao et al. in view of McAllister et al. and Hwang et al. as applied to claims 1-2, 4-5, and 7-9 above, and further in view of Lemieux (U.S. Pat. 6452942).

With respect to claim 6, the combination of Cao et al., McAllister et al., and Hwang et al. does not specifically disclose a step of label binding the first message for the second switch to a third switch.

Lemieux, in the field of communications, discloses using label binding to distribute information to other label switches in a network (**See column 5 line 45 to column 6 line 4 of Lemieux for reference to using label binding to distribute information to other label switches in a network**). Using label binding has the advantage of being able to explicitly map data to specific label switching paths.

It would have been obvious to one of ordinary skill in the art at the time of the invention, when presented with the work of Lemieux, to combine the label binding of Lemieux with the MPLS data network protection paths of Cao et al., McAllister et al., and Hwang et al., with the motivation being to be able to explicitly map data to specific label switching paths.

(10) Response to Argument

In response to Applicant's argument that there is no objective reason provided to combine the teachings of Cao et al. and McAllister et al. as proposed (See pages 8-9 of the Appeal Brief), the Examiner respectfully disagrees. First, it is noted that both Cao et al. and McAllister et al. deal with similar problems in similar environments. More specifically, both references deal with systems and methods of protection switching in network communication environments. The combination used in the rejections above is a combination of the MPLS system and method of setting up both working and protection paths through an MPLS network, as disclosed by Cao et al., with the protection switching control method, as disclosed by McAllister et al. Since both references deal with similar subject matter, it is not unreasonable for one of ordinary skill in the art to use the protection switching control method of McAllister et al. in the analogous network environment of Cao et al. The rationale to combine the teachings of McAllister et al. with those of Cao et al. comes from obvious advantages gained by using the protection switching control method of McAllister et al. that are not found in

Art Unit: 2616

the control method disclosed by Cao et al. It is pointed out that the motivation or rationale to combine does not necessarily need to be explicitly stated in the references themselves, but may also be implied by the references or found in the knowledge of one of ordinary skill in the art at the time of the invention. As stated in the rejections above, using a source switch to control protection switching provides the advantage of allowing a first, source, node to learn about a failure in a data path and immediately stop sending packets that will be "lost" on the failed path before the source node switches to the secondary path and also allowing the source node to resend packets on the secondary path that may have been "lost" while the destination node was receiving packets through the failed path. One of ordinary skill in the art at the time of the invention would have been familiar with this advantage of controlling protection switching from a source node.

In response to Applicant's argument the combination of the teachings of McAllister et al. with the teachings of Cao et al. would destroy the functionality of Cao et al. (See pages 9-10 of the Appeal Brief), the Examiner respectfully disagrees. As discussed above the combination used in the rejections is a combination of the MPLS system and method of setting up both working and protection paths through an MPLS network, as disclosed by Cao et al., with the protection switching control method, as disclosed by McAllister et al. Replacing the protection switching control method disclosed by Cao et al. with the protection switching control method of McAllister et al. would not change the other operations, such as the setting up of working and protection paths through an MPLS system, of the system disclosed by Cao et al. This

substitution of control methods does not improperly change the principle of operation of the system and method disclosed by Cao et al., as argued by the Applicant, since the rest of the system disclosed by Cao et al. would still operate in the same manner.

In response to Applicant's argument that a reasonable expectation of success has not been shown (See pages 10-11 of the Appeal Brief), the Examiner respectfully disagrees. As discussed above, replacing the protection switching control method disclosed by Cao et al. with the protection switching control method of McAllister et al. is possible and does not destroy the other teachings of Cao et al. Both references deal with the same problem of failure protection in a network environment and thus it would have been obvious for one of ordinary skill in the art to look at different types of failure protection control schemes when designing a failure protection system and method. The individual functions disclosed by Cao et al. and McAllister et al. would be not be changed in a system formed from the combined teachings as shown in the claim rejections.

In response to Applicant's argument that the combination of Cao et al. and McAllister et al. fails to disclose a third message sent over a reverse notification path indicating that received traffic was received on time and the interruption of which controls protections switching, as claimed (See pages 11-12 of the Appeal Brief), the Examiner respectfully disagrees. First, although Applicant argues that these limitations are not found within the teachings of Cao et al., this argument is moot since it is the teachings of McAllister et al. that are used to disclose these limitations in the rejection of the claims. McAllister et al. discloses sending constantly sending protocol messages or

data units from a node on one side of a link to a node on the other side of the link which must be acknowledged by the node on the other side of the link (See column 9 lines 53-56 of McAllister et al.). These messages are sent for each corresponding path of a call (See column 9 lines 56-64 of McAllister et al.). McAllister et al. also discloses that these the interruption of these messages is used to control protection switching (See column 9 line 56 to column 10 line 8 of McAllister et al.). Thus, these messages establish a reverse notification path for a corresponding call and their interruption controls protection switching at a source node. Further, since these messages are constantly sent and used to implement a keep-alive or heartbeat polling process for paths associated with a call, and their interruption indicates a failure of a path, the acknowledgement messages are an indication of whether the protocol messages or data units were received on time.

In response to Applicant's argument that the protocol and acknowledgement messages of McAllister et al. are sent on signaling paths separate from the data path (See pages 12-13 of the Appeal Brief), the Examiner respectfully disagrees. McAllister et al. discloses that the signaling links 38 used to transmit the protocol messages or data units and acknowledgements are a part of the data links 36 (See column 6 lines 20-40 and Figure 3 of McAllister et al.). As shown in Figure 3 of McAllister et al. a signaling link 38 is a logical bandwidth allocation of a part of the bandwidth allocated to a data link 36. Since the signaling link is part of the data link, the messages sent over a signaling link 38 inherently are also sent over a data link 36. Therefore, the protocol and acknowledgement messages of McAllister et al. are not sent on signaling paths

separate from the data path, as argued by the Applicant. Thus, using the acknowledgement messages to indicate whether the protocol messages or data units sent over the signaling link 38 were received on time does correspond to the claimed indicating whether a traffic flow sent on a working path was received on time, since the signaling link 38 is part of the data link 36.

In response to Applicant's argument that McAllister et al. does not disclose using the interruption of a third message to control protection switching by a first switch, as claimed (See page 13 of the Appeal Brief), the Examiner respectfully disagrees. McAllister et al. discloses that the interruption of the protocol messages and acknowledgement messages is used to indicate a failure and, in turn, to control a protection switching function at a source node (See column 9 lines 56 to column 10 line 8 of McAllister et al.). Thus, McAllister does disclose using the interruption of a third message (the acknowledgement message) to control protection switching by a first switch (the rerouting of the connection along a different path by the source node).

In response to Applicant's argument that Cao et al. would not be able to use the acknowledgement messages of McAllister et al. (See page 13 of the Appeal Brief), the Examiner respectfully disagrees. Again it is pointed out that the combination used in the rejections is a combination of the MPLS system and method of setting up both working and protection paths through an MPLS network, as disclosed by Cao et al., with the protection switching control method, as disclosed by McAllister et al. Since the protection switching control method disclosed by McAllister et al. performs protection

switching at the source node, the combined system of Cao et al. and McAllister et al. would also be able to perform protection switching at the source node.

In response to Applicant's argument that McAllister et al. fails to provide any traffic indication message indicating whether traffic was received on its data link on time (See pages 13-14 of the Appeal Brief), the Examiner respectfully disagrees. As discussed above, McAllister et al. discloses that the signaling links 38 used to transmit the protocol messages or data units and acknowledgements are a part of the data links 36 (See column 6 lines 20-40 and Figure 3 of McAllister et al.). Therefore, the protocol messages and acknowledgement messages sent over a signaling link are inherently data that is sent on a data link corresponding to the signaling link and do indicate whether that data was received on time.

In response to Applicant's argument that the functionality of Hwang et al. would make it incompatible with Cao et al. and McAllister et al. (See page 15 of the Appeal Brief), the Examiner respectfully disagrees. Hwang et al. discloses using an acknowledgement signal to indicate whether received data was received without errors (See column 7 lines 40-50 of Hwang et al.). Since McAllister et al. discloses using acknowledgement messages, it would have been obvious to adapt the acknowledgement messages of McAllister et al. to include the functionality of indicating whether data was received without errors, as disclosed by Hwang et al. This functionality is not incompatible with the teachings of Cao et al. and McAllister et al.

Art Unit: 2616

The Applicant's arguments regarding claims 3, 6, and 12 (See pages 16-18 of the Appeal Brief) do not include any further specific arguments not already discussed above.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.


Respectfully submitted,

Jason Mattis

Conferees:

Huy Vu

Ricky Ngo


HUY D. VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600


RICKY Q. NGO
SUPERVISORY PATENT EXAMINER